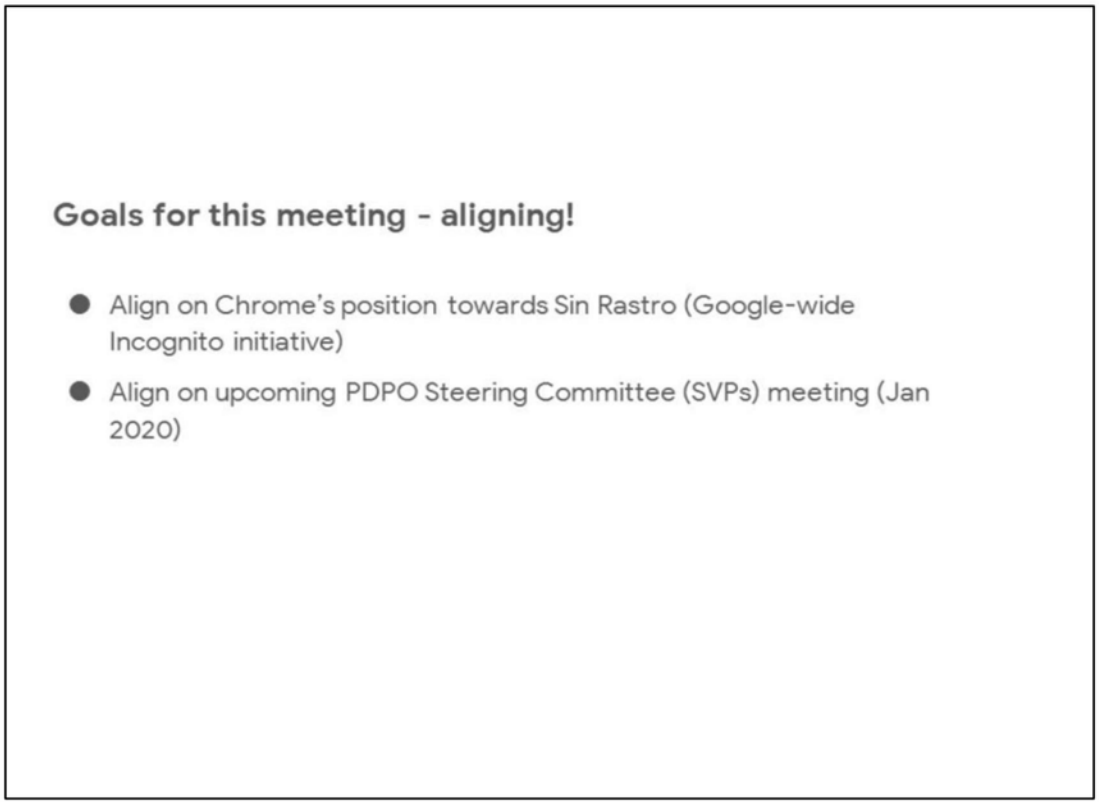
EXHIBIT 54

Redacted Version of Document Sought to be Sealed

Sin Rastro & Chrome | P.A.M. review

Chrome Privacy

Dec 2019



- Align on Chrome's position towards Sin Rastro (Google-wide Incognito initiative) in general, and in light of an upcoming PDPO Steering Committee meeting amongst a set of SVPs in particular.
- And prep them for Anil meeting

Quick recap

- Incognito in other Google products (xGA, YouTube, Maps) announced by Sundar at I/O 2019.
- Sin Rastro's mandate is to make the Incognito experience across Google products coherent and simpler to understand.
- Chrome's position is tough, as it's a Google product *and* a browser.

Id	Date	Text
1	12/11/2019 07:01:48	[redacted]


Current State
Strengthening Incognito story only client-side

- There are no incentives nor accountability for sites to offer a more private experience. They could already do that today.

Id	Date	Text
2	12/11/2019 06:44:43	May or may not be worth pointing out that this is more of a principled position as opposed to one that you see risks in (we previously discussed this when chatting about why Chrome believes that sites should not know Incognito state. This might help tee up option 2 in that we don't really see _abuse_ vectors (as opposed to comms/pr risks).

Current State | Public perception

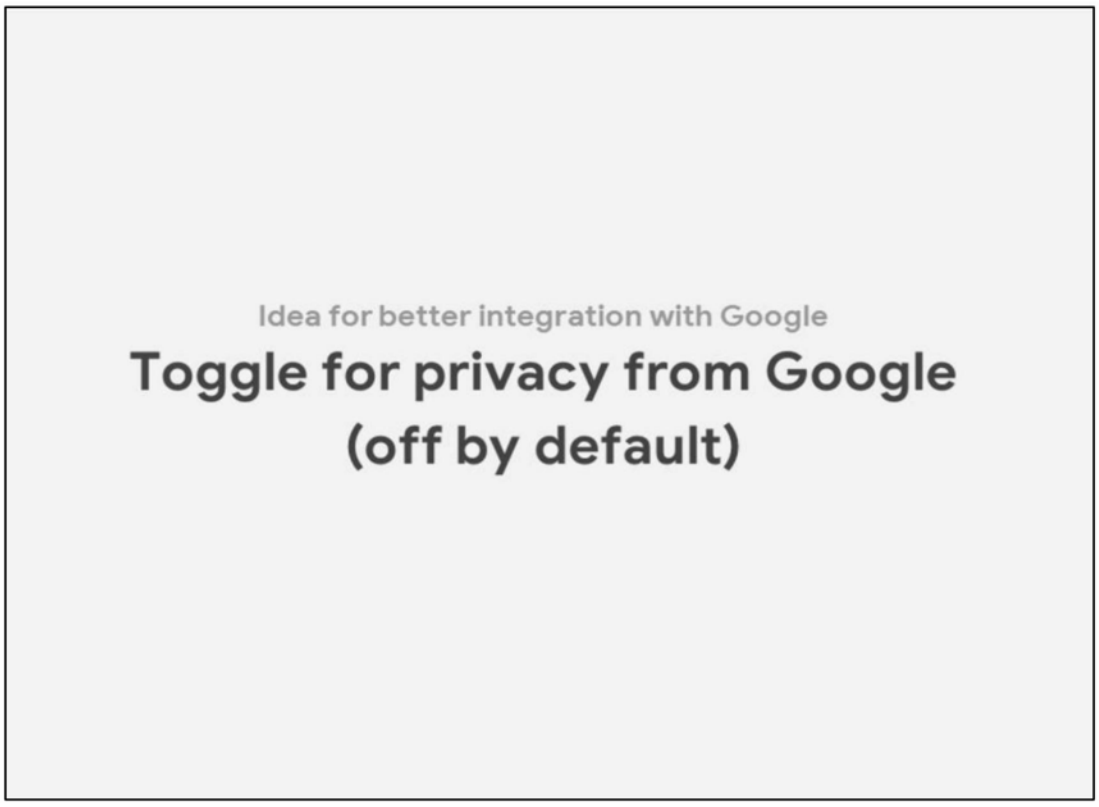
- We made recent PR statements that we won't tell websites when a user is in Incognito to prevent sites from abusing it.
- Significant public perception risks when flip-flopping on this (e.g., we linked this to domestic abuse and political oppression).
- PR said: "If we do that, we will be criticized as hypocrites 100%."

- Block 3rd party cookies by default in Incognito which prevents the most common tracking mechanisms.
- Inform user of long-running incognito sessions to make them more ephemeral.

Current State | Risks & impact on branding

- Sin Rastro Incognito story: Google doesn't collect personal information while in private mode. No personalization. No personal logs.
- Those guarantees aren't true in Chrome, which could lead to:
  - weaker overall privacy story
  - increased user confusion through different privacy guarantees in the YouTube, Maps, Search native apps vs. web apps
- Branding considers two separate brands in this case (though unlikely)

Id	Date	Text
3	12/11/2019 07:03:00	Potentially puts Chrome in an awkward position if 1p apps and their Incognito mode is more privacy protective than Chrome? We'd have to figure out how to tell that story.


Idea for better integration with Google
Toggle for privacy from Google
(off by default)

Toggle for Privacy from Google

- Toggle: *Use limited, privacy-focused versions of Google products.*
- When enabled, all supporting Google products run in their Incognito mode:
  - **Sign-in disabled.**
  - Distinct visual treatments.
  - More limited features and no in-session personalization for ads and products.
  - Support Incognito app transitions.
  - Nothing that requires consent (under GDPR and ePrivacy)
- (Edge and Bing are doing this.)

Id	Date	Text
1	12/11/2019 07:39:36	+sammit@google.com would this actually apply to all Google products? Or just Search/Maps/YT? _Reassigned to Sammit Adhya_
4	12/11/2019 07:39:36	So from a server-side perspective, we could all of it for zwieback keyed data. The infra is shared so that should be straight forward. The UX side is harder since each product outside of our flagships will need to implement the system. The goal of the design system is to make that easy.. but always will require some level of effort. Blocking sign in helps immensely as that limits us to the products that can be used while signed out.

Toggle for Privacy from Google | Pros

- Potential reduction of misconceptions due to different Incognito definitions.
- Provides more privacy from Google for those who want it.
- Users have the choice to have neutrality on the web.
- Doesn't break use cases like secret account.

Toggle for Privacy from Google | Risks

- Perception around toggle **being off by default**!
  - Hard to explain the reasoning behind it being off by default in a way that's convincing, not making regular mode look bad, and easy enough to understand.
  - The explanation would be around: not limiting the experience by default, supporting secret account, and developer use cases.

- No Google privacy on other browser or no promise for other websites
  - (This might not be possible anyway.)

Id	Date	Text
5	12/11/2019 07:43:46	Is this a con? Maybe this is where we can lean into the fact that Chrome is also a Google product (and tie it together with other initiatives that are Google-only)?

Where do we go from here?

If we accept considering this option,

- PDPO will work on a proposal based on this with all narratives, slogans, Google App changes, etc.

Appendix

Toggle on Incognito NTP, Main message

- Google offers better integration with its products and not even keeping your data *temporarily* to provide a customized experience.
- You can keep things as they are and always be treated as a *new user* in Chrome incognito.

Toggle text brainstorm

Toggle text:

- Use limited, privacy-focused versions of Google products.

- Use Google products in privacy-preserving mode
- Use Google products in a way that doesn't collect any personal information.
- Use restricted/limited versions of Google products that don't collect any personal information.
- Turn on some benefits with some drawbacks.
- Trade some features for privacy.
- Turn on something that Firefox doesn't have.

Some negative narratives...

- "The truth is that private browsing is as private as our playing a video with the sound on at the airport."
- "But it doesn't do much to protect your privacy. Your ISP can see what websites you visit, and services like Twitter can figure out who you are even without cookies."
- "YouTube Incognito sessions influence home feed recommendations, despite Google's claims that they're private"
- "A new incognito mode on Google Maps may make it easier to obscure your search history. But that doesn't mean the app won't be tracking your whereabouts."
- "Google Chrome's Incognito Mode is way less private than you think"
- "Despite the long-known fact that Incognito isn't truly anonymous, new research has re-emphasised that Google and other web browsers are still tracking you in privacy mode, even on the most sensitive of sites."
- "That is, while in Incognito mode, Google is still tracking your searches, and can use them to send intrusive ads at you across the Web on the millions of sites and apps that run Google ads. Sure, your search or browser history won't be on your computer, but Google still knows it. And when you get served an ad based on that "incognito" search you did recently (like, let's say that surprise vacation you were planning), it's not so private anymore."
- Articles

Bing!